Supreme Court, U.S.
FILED
DEC 29 1988
JOSEPH F. SPANIOL, JR.
CLERK

No. 87-2127

IN THE

Supreme Court of the United States

OCTOBER TERM, 1988

AMERICAN FOREIGN SERVICE ASSOCIATION, *et al.*,
Appellants,

v.

STEVEN GARFINKEL, *et al.*,
Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

JOINT APPENDIX

Patti A. Goldman
Counsel of Record
Alan B. Morrison
Paul Alan Levy
Public Citizen Litigation Group
Suite 700
2000 P Street, N.W.
Washington, D.C. 20036
(202) 785-3704

Susan Holik
American Foreign Service Association
2101 E Street, N.W.
Washington, D.C. 20037
(202) 647-8160

Attorneys for Appellants

Charles Fried
Solicitor General
John R. Bolton
Assistant Attorney General
Thomas Merrill
Deputy Solicitor General
Edwin S. Kneedler
Assistant to the Solicitor General
Barbara L. Herwig
Freddi Lipstein
Attorneys
Department of Justice
Washington, D.C. 20530
(202) 633-2217

Attorneys for Appellees

THE COURT NOTED PROBABLE JURISDICTION ON OCTOBER 31, 1988.

TABLE

Docket Entries 1

Complaint filed February 19, 1988 5

Plaintiffs' Exhibit 2 — National Security Decision Directive 84 (March 11, 1983). 11

Plaintiffs' Exhibit 3 — Standard Form 189 15

Plaintiffs' Exhibit 5 — Standard Form 4193 19

Plaintiffs' Exhibit 6 — Declaration of Lt. General Edward J. Heinz (Feb. 9, 1988), in *National Federation of Federal Employees v. United States*, No. 87-2284-OG & *American Federation of Government Employees v. Garfinkel*, No. 87-2412-OG (D.D.C.). 26

Plaintiffs' Exhibit 7 — Affidavit of Steven Garfinkel (Feb. 8, 1988), in *National Federation of Federal Employees v. United States*, No. 87-2284-OG & *American Federation of Government Employees v. Garfinkel*, No. 87-2412-OG (D.D.C.). 28

Plaintiffs' Exhibit 8 — Information Security Oversight Office Letter of December 29, 1987. 30

Plaintiffs' Exhibit 9 — Information Security Oversight Office Letter of January 27, 1988. 32

Plaintiffs' Exhibit 10 — Affidavit of Representative Barbara Boxer (Nov. 17, 1987). 34

Plaintiffs' Exhibit 11 — Affidavit of Senator Charles E. Grassley (Nov. 18, 1987). 37

Defendants' Exhibit 4 — Declaration of William H. Webster, Director of Central Intelligence (Mar. 1, 1988). 40

Exhibit A in Support of the Declaration of William H. Webster —DCI Security Committee, Sensitive Compartmented Information: Characteristics and Security Requirements (June 1984). 45

Declaration of Lt. General Edward J. Heinz (Mar. 24, 1988). 52

Exhibit A in Support of Lt. General Heinz's Declaration — Standard Form 4355 54

Plaintiffs' Exhibit 16 — Letter to Chairman Jack Brooks from Colin L. Powell, National Security Council (Mar. 8, 1988). 59

Opinion and Order (May 27, 1988)(reproduced in appendix to jurisdictional statement). x

Notice of Appeal (June 3, 1988)(reproduced in appendix to jurisdictional statement). x

Final Judgment and Order, *National Federation of Federal Employees v. United States*, No. 87-2284-OG (D.D.C. July 29, 1988) & *American Federation of Government Employees v. Garfinkel*, No. 87-2412-OG (D.D.C.). 61

Order, *National Federation of Federal Employees v. United States*, No. 87-2284-OG (D.D.C. Sept. 26, 1988) & *American Federation of Government Employees v. Garfinkel*, No. 87-2412-OG (D.D.C.). 64

Standard Form 312 66

DOCKET ENTRIES

2/19/88	1	COMPLAINT filed summons issued (ew) [Entry date 2/22/88]
2/19/88	2	MOTION by plaintiff for preliminary injunction; Exhibits (15) (ew) [Entry date 2/22/88]
2/23/88	3	NOTICE OF FILING by plaintiffs Re: responses to interrogatories and request for production of documents submitted by defendants in the related cases CA 87-2284 and CA 87-2412 (gld) [Entry date 2/24/88]
2/26/88	4	ATTORNEY APPEARANCE for defendant GEORGE P. SHULTZ, defendant WILLIAM H. WEBSTER, defendant STEVEN GARFINKEL by David Anderson, Vincent M. Garvey, Neal Dittersdorf, William Robert Irvin (gld) [Entry date 2/29/88]
2/26/88	5	MOTION by defendant GEORGE P. SHULTZ, defendant WILLIAM H. WEBSTER, defendant STEVEN GARFINKEL to extend time to 3/2/88 to file opposition to plaintiffs motion for preliminary injunction (gld) [Entry date 2/29/88]
3/4/88	6	ORDER by Judge Oliver Gasch: granting motion by defendants to extend time to 3/2/88 to file opposition to plaintiffs motion for preliminary injunction [5-1] (signed 3/3/88) (N) (gld) [Entry date 3/8/88]
3/4/88	7	MOTION by GEORGE P. SHULTZ, defendant WILLIAM H. WEBSTER, defendant STEVEN

GARFINKEL for leave to file a reply brief and memorandum in support (gld) [Entry date 3/8/88]

3/4/88 8 AFFIDAVIT OF SERVICE of summons and complaint upon defendant GEORGE P. SHULTZ (unexecuted); upon defendant WILLIAM H. WEBSTER (unexecuted); upon defendant STEVEN GARFINKEL on 2/22/88; upon U.S. Attorney on 2/19/88; Attachments (gld) [Entry date 3/8/88]

3/8/88 — STATUS HEARING before Judge Oliver Gasch: oral motion by govt. to consolidate this action with CA 87-2284 and 87-2412 heard; hearing on motion for preliminary injunction [2-1] by plaintiff set for 10:00 a.m., on 4/14/88 reporter F. Rangus (gld) [Entry date 3/10/88]

3/9/88 — ALL PLEADINGS FILED AFTER 3/9/88 WILL BE FILED AND DOCKETED IN THE LEAD CASE 87-2284 (kc) [Entry date 3/14/88]

3/9/88 11 ORDER by Judge Oliver Gasch: granting status hearing oral motion by government to consolidate CA 88-440 with CA 87-2284 and 87-2412 (N) (kc) [Entry date 3/14/88]

3/10/88 9 REPLY MEMORANDUM by plaintiffs in support of motion for preliminary injunction [2-1] by plaintiff (gld) [Entry date 3/11/88]

3/11/88 10 MEMORANDUM by defendant GEORGE P. SHULTZ, defendant WILLIAM H. WEBSTER, defendant STEVEN GARFINKEL in opposition to motion for preliminary injunction [2-1]

by plaintiff; Exhibits (fiat) GASCH, J. (gld) [Entry date 3/14/88]

3/21/88 12 MOTION by plaintiffs in 1:88-cv-00440 for summary judgment (kc) [Entry date 3/23/88]

3/30/88 13 ORDER by Judge Oliver Gasch: granting motion for leave to file motion to dismiss second amended complaints with P&A's in excess of page limitation [44-1] in 1:87-cv-02284 (N) (kc) [Entry date 3/31/88]

4/6/88 14 ORDER by Judge Oliver Gasch: granting motion to extend time to file their reply brief in support of their motion for summary judgment [49-1] in 1:87-cv-02284 (N) (kc) [Entry date 4/11/88]

4/11/88 15 MEMORANDUM by plaintiffs Public Citizen Litigation Group in 1:88-cv-00440 in opposition to motion to dismiss [47-1] by defendant in 1:87-cv-02284 (kc) [Entry date 4/12/88]

4/21/88 — MOTION HEARING by defendant motion to dismiss [47-1] by NATL. FEDERATION and motion for preliminary injunction [37-1] taken under advisement; parties to file proposed findings and conclusions within ten (10) days in 1:87-cv-02284 before Judge Oliver Gasch: reporter E. Olsen (kc) [Entry date 4/22/88]

5/27/88 16 MEMORANDUM OPINION by Judge Oliver Gasch (N) (kc) [Entry date 6/7/88]

5/27/88 17 ORDER by Judge Oliver Gasch: denying motion for preliminary injunction [37-1] by NATL.

FEDERATION FED in 1:87-cv-02284, granting motion for summary judgment [38-1] in 1:87-cv-02284, denying motion for summary judgment 1:88-cv-00440, granting in part, denying in part motion to dismiss [47-1]; directing that counts I and III of the complaint are dismissed in CA 87-2284; directing that Counts III, IV, VI, VIII, IX, XI, XII, and XIII of the Complaint in CA 87-2412 are dismissed. CASE CLOSED AS TO CA 88-0440 ONLY in 1:87-cv-02284 (N) (kc) [Entry date 6/7/88]

6/3/88 ENTERED IN ERROR NOTICE OF APPEAL by plaintiff in 1:88-cv-00440 from order [17-1]; $5.00 filing paid. $100.00 Docketing fee not paid. Copies mailed to Wm. Robert Irvin, Freddi Lipstein and Solicitor General (kc) [Entry date 6/7/88 [Edit date 6/29/88]

6/3/88 19 NOTICE OF APPEAL by plaintiff in 1:88-cv-00440 to Supreme Court from order [17-1] $5.00 filing fee paid (kc) [Entry date 6/28/88]

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AMERICAN FOREIGN SERVICE ASSOCIATION,
2101 E Street, N.W.
Washington, D.C. 20037,
REPRESENTATIVE JACK BROOKS,
Washington, D.C. 20515,
REPRESENTATIVE BARBARA BOXER,
Washington, D.C. 20515,
SENATOR CHARLES GRASSLEY,
Washington, D.C. 20510,
SENATOR WILLIAM PROXMIRE
Washington, D.C. 20510,
SENATOR DAVID PRYOR,
Washington, D.C. 20510,
REPRESENTATIVE PAT SCHROEDER,
Washington, D.C. 20515,
and
REPRESENTATIVE GERRY SIKORSKI,
Washington, D.C. 20515,
Plaintiffs,
v.
STEVEN GARFINKEL, DIRECTOR,
Information Security Oversight
Office,
18th & F Streets, N.W., Room 6046
Washington, D.C. 20405,
WILLIAM H. WEBSTER,
Director of Central Intelligence,
Washington, D.C. 20505,
and
GEORGE P. SHULTZ,
Secretary of State,
2201 C Street, N.W., 7th Floor
Washington, D.C. 20520,
Defendants.

88–0440
Feb 19, 1988
Gasch, J.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. This action seeks declaratory and injunctive relief from defendants' continued use of two standard nondisclosure forms in violation of Section 630 of the Continuing Resolution for Fiscal Year 1988, Pub. L. No. 100-202, 100th Cong., 1st Sess. (Dec. 22, 1987)("Continuing Resolution") and the Administrative Procedure Act, 5 U.S.C. § 706.

2. This Court has jurisdiction under 28 U.S.C. § 1331.

PARTIES

3. Plaintiff American Foreign Service Association is a professional and labor association of foreign service employees, and is the certified bargaining representative for employees of the State Department. Most of its members have access to classified information, and many of them have access to Sensitive Compartmented Information. It has members who have signed Standard Form ("SF 4193") both before and after December 22, 1987, and who continue to be faced with its obligations and possible enforcement of its terms in respects not authorized by law. Since December 22, 1987, its members who are employed by the State Department have been required, and are still being required, to sign SF 4193.

4. Plaintiffs Charles Grassley, William Proxmire, and David Pryor are United State Senators, who rely on information furnished by federal employees in order to carry out their duties as Senators.

5. Plaintiffs Barbara Boxer, Jack Brooks, Pat Schroeder, and Gerry Sikorski are United States Representatives, who rely on information furnished by federal employees in order to carry out their duties as Representatives.

6. Defendant Steven Garfinkel is the Director of the Information Security Oversight Office ("ISOO"), and is responsible for overseeing compliance with the security classification system set forth in Executive Order 12,356, § 5.2, for implementing the requirement of National Security Decision Directive 84 ("NSDD-

84") that employees must sign a nondisclosure agreement as a condition of access to classified information, and for developing standard nondisclosure forms. Exec. Order 12,356, § 5.2(b)(7); NSDD-84 ¶ 1(c).

7. Defendant William H. Webster is the Director of Central Intelligence ("DCI") and is responsible under Executive Order 12,356, § 4.2(a), and 50 U.S.C. § 403(d)(3), for promulgating policies for the security, use, and dissemination of classified information concerning nondisclosure intelligence sources or methods, which is known as Sensitive Compartmented Information ("SCI"), including policies concerning nondisclosure agreements for those who have access to SCI.

8. Defendant George P. Shultz is the Secretary of State and the head of the State Department, a federal agency with employees who have access to classified information, including SCI, which has required its employees to sign SF 4193 since December 22, 1987.

BACKGROUND

9. On March 11, 1983, President Ronald Reagan issued NSDD- 84, which directs that all persons with access to classified information must sign approved nondisclosure agreements as a condition of access and which makes the Director of ISOO responsible for developing forms for this purpose.

10. In 1983, defendant Garfinkel issued Standard Form 189 ("SF 189") in accordance with NSDD-84's requirement and directed all agencies to require their employees who have access to classified information to sign SF 189.

11. Defendant Webster's predecessor approved SF 4193 in December 1981, and subsequently required all federal employees with access to SCI to sign SF 4193.

12. On December 22, 1987, the President signed the Continuing Resolution for Fiscal Year 1988. Section 630 thereof provides that "[n]o funds appropriated in this resolution or any other Act for fiscal year 1988 may be used to implement or enforce the agreements in Standard Forms 189 and 4193 of the Government or any other nondisclosure policy, form or agreement" that

contains any of five specified provisions, all of which are included in SF 189 and SF 4193.

13. After the President signed the Continuing Resolution, defendant Webster has continued to require employees with access to SCI to sign SF 4193 but has directed that during Fiscal Year 1988 SF 4193 should be accompanied by an addendum that states that "[t]he obligations imposed by this Agreement shall be implemented and enforced in a manner consistent with the [Continuing Resolution]." At his direction, Lt. General Edward J. Heinz, the Director of Intelligence Community Staff, has stated in a declaration filed in a related case that a refusal to sign SF 4193 will result in a denial of access to SCI.

14. By letter dated December 29, 1987, defendant Garfinkel directed 69 federal agencies to stop requiring their employees to sign SF 189.

15. By letter dated January 27, 1988, defendant Garfinkel advised the same 69 federal agencies to treat SF 189 agreements executed on or after December 22, 1987, as voidable at the behest of the employee.

16. Defendant Garfinkel has issued no other directions to federal agencies regarding compliance with the Continuing Resolution.

17. After December 22, 1987, defendant Shultz has required, and is still requiring, State Department employees who have access to SCI to sign SF 4193.

18. Plaintiffs are irreparably injured by defendants' failure to comply with the Continuing Resolution because SF 4193 and SF 189 chill employees' constitutional and statutory rights to free speech and to petition Congress, and they impede the congressional plaintiffs' ability to obtain important information from federal employees, which they need to carry out their duties.

CAUSES OF ACTION

COUNT I (Continued Implementation)

19. By requiring federal agencies to have their employees sign SF 4193 after December 22, 1987, defendant Webster has

violated Section 630 of the Continuing Resolution and acted contrary to law within the meaning of the Administrative Procedure Act, 5 U.S.C. § 706.

COUNT II (Continued Implementation)

20. By requiring State Department employees to sign SF 4193 after December 22, 1987, defendant Shultz has violated Section 630 of the Continuing Resolution and acted contrary to law within the meaning of the Administrative Procedure Act, 5 U.S.C. § 706.

COUNT III (Continued Implementation)

21. By directing federal agencies to cease execution of SF 189, but advising them that all such agreements executed after December 22, 1987, are voidable at the behest of the employees, and not simply void, and by failing to tell such agencies that they should notify all employees who signed SF 189 after December 22, 1987, that such agreements are void, defendant Garfinkel acted arbitrarily and capriciously and not in accordance with law in violation of the APA, 5 U.S.C. § 706.

COUNT IV (Continued Enforcement)

22. By not requiring federal agencies to notify employees who signed SF 189s and SF 4193s both prior to and subsequent to December 22, 1987, that the five terms specified in the Continuing Resolution cannot be enforced during Fiscal Year 1988, defendants Webster and Garfinkel have violated the Continuing Resolution's ban on enforcement and have acted arbitrarily, capriciously, and contrary to law within the meaning of the Administrative Procedure Act, 5 U.S.C. § 706.

WHEREFORE, plaintiffs pray that this Court:

(1) Enter an order declaring

(A) that, by directing federal agencies to continue requiring individuals to sign SF 4193 after December 22, 1987, defendant Webster violated Section 630 of the Continuing Resolution and acted contrary to law within the meaning of the Administrative Procedure Act, 5 U.S.C. § 706;

(B) that, be requiring State Department employees and officers to sign SF 4193 after December 22, 1987, defendant

Shultz violated Section 630 of the Continuing Resolution and acted contrary to law within the meaning of the Administrative Procedure Act, 5 U.S.C. § 706; and

(C) that all SF 189 and SF 4193 agreements executed after December 22, 1987, are void;

(2) Enter a preliminary and permanent injunction

(A) enjoining defendant Shultz from requiring State Department employees and officers to sign SF 4193 during the remainder of Fiscal Year 1988;

(B) directing defendant Shultz to treat all SF 4193 agreements executed on or after December 22, 1987, as void, and to notify all State Department signatories that such agreements are void;

(C) directing defendants Garfinkel and Webster to prohibit federal agencies from requiring federal employees and officers to sign SF 4193 during the remainder of Fiscal Year 1988; and

(D) directing defendants Garfinkel and Webster to require federal agencies to treat all SF 189 and SF 4193 agreements executed after December 22, 1987, as void, and to notify all of the signatories of such agreements that they are void;

(3) Enter an order directing defendants Garfinkel and Webster to require federal agencies to notify all employees who have signed SF 189 and/or SF 4193 at any time that the five terms specified in the Continuing Resolution may not be enforced during Fiscal Year 1988;

(4) Award plaintiffs their costs and reasonable attorneys' fees in this action, pursuant to the Equal Access to Justice Act, 28 U.S.C. § 2412(d); and

(5) Grant such other and further relief as this Court may deem just and proper.

Respectfully submitted,

/s/

Pl. Exhibit 2

THE WHITE HOUSE
WASHINGTON

National Security Decision Directive Number 84
March 11, 1983

Safeguarding National Security Information

As stated in Executive Order 12356, only that information whose disclosure would harm the national security interests of the United States may be classified. Every effort should be made to declassify information that no longer requires protection in the interest of national security.

At the same time, however, safeguarding against unlawful disclosures of properly classified information is a matter of grave concern and high priority for this Administration. In addition to the requirements set forth in Executive Order 12356, and based on the recommendations contained in the interdepartmental report forwarded by the Attorney General, I direct the following:

1. Each agency of the Executive Branch that originates or handles classified information shall adopt internal procedures to safeguard against unlawful disclosures of classified information. Such procedures shall at a minimum provide as follows:

a. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. This requirement may be implemented prospectively by agencies for which the administrative burden of compliance would otherwise be excessive.

b. All persons with authorized access to Sensitive Compartmented Information (SCI) shall be required to sign a

nondisclosure agreement as a condition of access to SCI and other classified information. All such agreements must include a provision for prepublication review to assure deletion of SCI and other classified information.

c. All agreements required in paragraphs 1.a. and 1.b. must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States. The Director, Information Security Oversight Office (IS00), shall develop standardized forms that satisfy these requirements.

d. Appropriate policies shall be adopted to govern contacts between media representatives and agency personnel, so as to reduce the opportunity for negligent or deliberate disclosures of classified information. All persons with authorized access to classified information shall be clearly apprised of the agency's policies in this regard.

2. Each agency of the Executive branch that originates or handles classified information shall adopt internal procedures to govern the reporting and investigation of unauthorized disclosures of such information. Such procedures shall at a minimum provide that:

a. All such disclosures that the agency considers to be seriously damaging to its mission and responsibilities shall be evaluated to ascertain the nature of the information disclosed and the extent to which it had been disseminated.

b. The agency shall conduct a preliminary internal investigation prior to or concurrently with seeking investigative assistance from other agencies.

c. The agency shall maintain records of disclosures so evaluated and investigated.

d. Agencies in the possession of classified information originating with another agency shall cooperate with the originating agency by conducting internal investigations of the unauthorized disclosure of such information.

e. Persons determined by the agency to have knowingly made such disclosures or to have refused cooperation with investigations of such unauthorized disclosures will be denied further access to classified information and subjected to other administrative sanctions as appropriate.

3. Unauthorized disclosures of classified information shall be reported to the Department of Justice and the Information Security Oversight Office, as required by statute and Executive orders. The Department of Justice shall continue to review reported unauthorized disclosures of classified information to determine whether FBI investigation is warranted. Interested departments and agencies shall be consulted in developing criteria for evaluating such matters and in determining which cases should receive investigative priority. The FBI is authorized to investigate such matters as constitute potential violations of federal criminal law, even though administrative sanctions may be sought instead of criminal prosecution.

4. Nothing in this directive is intended to modify or preclude interagency agreements between FBI and other criminal investigative agencies regarding their responsibility for conducting investigations within their own agencies or departments.

5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies, as necessary, so that employees may be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information. As a minimum, such regulations shall permit an agency to decide that appropriate adverse consequences will follow an employee's refusal to cooperate with a polygraph examination that is limited in scope to the circumstances of the unauthorized disclosure under investigation. Agency regulations may provide that only the head of the agency, or his delegate, is empowered

to order an employee to submit to a polygraph examination. Results of polygraph examinations should not be relied upon to the exclusion of other information obtained during investigations.

6. The Attorney General, in consultation with the Director, Office of Personnel Management, is requested to establish an interdepartmental group to study the federal personnel security program and recommend appropriate revisions in existing Executive orders, regulations, and guidelines.

/s/ Ronald Reagan

Pl. Exhibit 3

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security

clearance that such disclosure is permitted. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised and am aware that any unauthorized disclosure of classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials which have, or may have, come into my possession or for which I am

responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798 and 952 of Title 18, United States Code, Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356, so that I may read them at this time, if I so choose.

11. I make this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. (See notice below)
ORGANIZATION		

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE
ORGANIZATION	

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that all federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

STANDARD FORM 189 (8/83)
Prescribed by GSA/ISOO
32 CFR 2003:E.O. 12356

Pl. Exhibit 5

SENSITIVE COMPARTMENTED INFORMATION NON-DISCLOSURE AGREEMENT

An Agreement Between _____ and the United States

(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or classifiable under the standards of Executive Order 12065 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge such information to anyone who is not authorized

to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I further understand that I am obligated by law and regulation not to disclose any classified information in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information, all information or materials, including works of fiction, which contain or purport to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such information and materials for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the information or materials with, or showing them to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose such information or materials to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the information or materials submitted pursuant to paragraph 4 set forth any SCI. I further understand that the Department or Agency to which I have submitted materials will act upon them, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and retention in a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials, which may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed upon by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12065, as amended, so that I may read them at this time, if I so choose.

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. I make this Agreement without any mental reservation or purpose of evasion.

_____ _____

SIGNATURE DATE

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented

Information.

WITNESS and ACCEPTANCE:

SIGNATURE _____ DATE _____

SECURITY BRIEFING ACKNOWLEDGMENT

I hereby acknowledge that I was briefed on the following SCI Special Access Program(s):

_____

(Special Access Programs by Initials Only)

_____ _____

Signature of Individual Briefed Date Briefed

_____

Printed or Typed Name

_____ _____

Social Security Number (See Notice Below) Organization (Name nd Address)

I certify that the above SCI access(es) were approved in accordance with relevant SCI procedures and that the briefing presented by me on the above date was also in accordance therewith.

_____

Signature of Briefing Officer

_____

Printed or Typed Name

_____ _____

Social Security Number (See Notice Below) Organization (Name and Address)

SECURITY DEBRIEFING ACKNOWLEDGMENT

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the following SCI Special Access Program(s):

_____

(Special Access Programs by Initials Only)

_____ _____

Signature of Individual Briefed Date Briefed

_____

Printed or Typed Name

_____ _____

Social Security Number (See Notice Below) Organization (Name and Address)

I certify that the debriefing presented by me on the above date was in accordance with relevant SCI procedures.

_____

Signature of Briefing Officer

_____

Printed or Typed Name

_____ _____

Social Security Number (See Notice Below) Organization (Name and Address)

NOTICE: The Privacy Act, 5 U.S.C. § 522a, [sic] requires that all federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Ac-

count Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

Form 4193 12/81	Obsolete Previous Edition	(Replace Forms 4066, 3968, 4193a and 4193b which are obsolete and will not be used)

Pl. Exhibit 6

[Caption]

DECLARATION OF LT. GENERAL EDWARD J. HEINZ

I, LT. GENERAL EDWARD J. HEINZ, USAF, declare as follows:

1. I am the Director of the Intelligence Community Staff, which is a staff element of the Director of Central Intelligence (DCI) that was created under the authority of Executive Order 12333. I submit this Declaration pursuant to the Court's Order of February 2, 1988.

2. Pursuant to Section 102(d) of the National Security Act of 1947, 50 U.S.C. § 403(d)(3), and Executive Order 12356, the Director of Central Intelligence (DCI) is responsible for promulgating policies and procedures for the security, use, and dissemination of Sensitive Compartmented Information (SCI). SCI is classified information, concerning or derived from intelligence sources, methods or analytical processes, which is required to be handled within formal access control systems established by the DCI.

3. In my capacity as Director of the Intelligence Community Staff, I am responsible for assisting the DCI in establishing security policy with respect to SCI. The DCI has directed that the signing of a DCI-authorized nondisclosure agreement is a condition of access to SCI and has made available Form 4193 ("Sensitive Compartmented Information Nondisclosure Agreement") for Government-wide use for this purpose. I am responsible for the administration and implementation of Form 4193 throughout the Government.

4. In response to Section 630 of the Omnibus Continuing Resolution for FY 1988, Public Law 100-202, I am reviewing, in consultation with the Department of Justice, the continued use of Form 4193 and am considering whether to revise Form 4193 in light of this legislation. Meanwhile, in order to ensure that implementation and enforcement of nondisclosure agreements

that protect SCI will be consistent with Section 630, I have issued instructions to all departments, agencies and offices responsible for SCI indoctrinations and debriefings. I have directed that, during Fiscal Year 1988, Form 4193, and any other nondisclosure agreements used for the protection of SCI, shall only be used when accompanied by a special addendum which states:

> The obligations imposed by this Agreement shall be implemented and enforced in a manner consistent with the section entitled "Employee Disclosure Agreements" contained in P.L. 1000-202, [sic] Continuing Appropriations for Fiscal Year 1988, 22 December 1987, and other applicable law.

A copy of Form 4193 accompanied by the special addendum is attached hereto as Exhibit A. Refusal of the person seeking access to SCI to sign an SCI nondisclosure form, as modified by the special addendum, will result in denial of access to SCI.

5. I declare under penalty of perjury that the foregoing is true to the best of my belief.

/s/ Edward J. Heinz
Edward J. Heinz, Lt. General, USAF

Date: 9 Feb 1988

The obligations imposed by this Agreement shall be implemented and enforced in a manner consistent with the section entitled "Employee Disclosure Agreements" contained in P.L. 100-202, Continuing Appropriations for Fiscal Year 1988, 22 December 1987, and other applicable law.

Witness Signature	Signature
Date: _____	Date: _____

Pl. Exhibit 7

[Caption]

AFFIDAVIT OF STEVEN GARFINKEL

I, Steven Garfinkel, Director, Information Security Oversight Office, being duly sworn, hereby make the following statement:

1. I have served as Director of the Information Security Oversight Office (ISOO) since May 1980. Under Executive Order 12356, "National Security Information," the ISOO Director is responsible to the President for overseeing the security classification system throughout the executive branch, and for reporting to the President annually on the status of that program. Further, under National Security Decision Directive 84, signed by the President on March 11, 1983, the ISOO Director is responsible for implementing a standardized nondisclosure agreement between individuals and the United States to be executed as a condition of access to classified information. In fulfilling this responsibility, on September 9, 1983, I issued the Standard Form 189, "Classified Information Nondisclosure Agreement" (SF 189). Following the issuance of the SF 189, I oversaw its implementation throughout the executive branch.

2. Following the Congress' passage of the Continuing Resolution for Fiscal Year 1988 (Public Law 100-202), I learned that it contained language that possibly affected the use of appropriated funds during the remainder of FY 1988 to implement and enforce the SF 189. I determined that the best course of action for ISOO to take with respect to the SF 189 was to suspend its further implementation, at least until I had received a formal opinion of the Attorney General or his representative on the impact of the enacted legislation. Accordingly, on December 29, 1987, I delivered or mailed a letter to the senior agency official for the information security program of 69 departments, agencies, or independent offices that create or handle national security information. Among other instructions, the letter directed each agency pending further instructions to "[c]ease any addi-

tional implementation of [the August 1983 edition] of the SF 189 . . .." A copy of my letter of December 29, 1987, is attached to this affidavit as Exhibit A. The names and addresses of the officials to whom I addressed this letter are attached to this affidavit as Exhibit B.

3. On January 27, 1988, I delivered or mailed another letter to the officials listed in Exhibit B to supplement my instructions contained in the letter of December 29, 1987. The second letter directed agencies to ". . . take reasonable steps to notify all affected employees that until further notice [the agencies] will treat an SF 189 . . . executed on or after December 22, 1987, as voidable at the behest of the employee who signed it." A copy of my letter of January 27, 1988, is attached to this affidavit as Exhibit C.

4. Since my letter of January 27, 1988, I have issued no further instructions nor propounded any further policy with respect to the implementation of the SF 189. I have read the statement above, consisting of three pages, and declare, under penalty of perjury, that it is true and complete to the best of my knowledge and belief.

/s/ Steven Garfinkel
Steven Garfinkel

[Notarized]

Pl. Exhibit 8

EXHIBIT A

Information Security Oversight Office
Washington, D.C. 20405

COPY

December 29, 1987

Dear (Salutation):

A last minute rider to the Continuing Resolution for Fiscal Year 1988 (Section 630 of Public Law 100-202, copy enclosed), passed by Congress on December 21, and signed by the President on December 22, 1987, places limitations on the implementation and enforcement of the Standard Form 189, "Classified Information Nondisclosure Agreement." The Information Security Oversight Office (ISOO) will seek an Opinion of the Attorney General on the impact if this legislation on the SF 189 and the SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/ Commercial/Non-Government)." In the interim, and pending further instructions, please implement the following actions at once, including immediate notification to all affected subordinate activities:

1. Cease any additional implementation of existing editions of the SF 189 and SF 189-A. That is, do not have any other personnel execute the August 1983 edition of SF 189, or the June 1986 edition of SF 189-A. ISOO intends to issue as quickly as possible revised editions of each form. You will be provided further instructions as they become available.

2. Do not destroy any existing executed copies of SF 189 and SF 189-A. If at all possible, ISOO will seek to maintain their validity to the extent that they are consistent with the language of Pub. L. 100-202 and revised editions of the forms.

3. Continue the moratorium on any action against a cleared individual who has refused to execute SF 189 in the past. In all likelihood, this moratorium will be lifted when new editions of the nondisclosure agreements are available.

4. Brief cleared unsigned personnel fully on their obligations to protect classified information, and on the sanctions that may result from unauthorized disclosures.

5. Take all appropriate sanctions against personnel who disclose classified information without authority, whether they have signed a nondisclosure agreement or not. Consult with agency counsel, Justice Department counsel, or ISOO concerning the enforceability of executed nondisclosure agreements in taking such actions.

Please contact your ISOO liaison or me at FTS 535-7251 (commercial (202) 535-7251), if you have any questions.

Sincerely,

/s/ Steven Garfinkel

Steven Garfinkel
Director

Pl. Exhibit 9

EXHIBIT C
Information Security Oversight Office
Washington, D.C. 20405
January 27, 1988 COPY

Dear (Salutation):

On December 29, 1987, the Information Security Oversight Office (ISOO) provided interim instructions to your agency concerning the implementation and enforcement of the Standard Form 189, "Classified Information Nondisclosure Agreement," and the SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)," in response to Sec. 630 of Public Law 100-202, the Continuing Resolution for FY 1988. Among these instructions were the requirements to cease the execution by employees of the current editions of SF 189 or SF 189-A, and to retain all existing signed copies of the agreements. This letter supplements those instructions by addressing the handling of those nondisclosure agreements that are dated on or after December 22, 1987; that is, those that are executed between the day that the President signed the Continuing Resolution into law and the time that agency and contractor units receive and carry out the instruction to halt implementation.

At this time the enforceability of these agreements is unclear, and ISOO will seek the advice of the Justice Department on this issue. In the interim, however, agencies shall take reasonable steps to notify all affected employees that until further notice they will treat an SF 189 or SF 189-A executed on or after December 22, 1987, as voidable at the behest of the employee who signed it. At the request of an employee, the agency must take action to void this particular written agreement. The

employee shall then be considered as a cleared non-signatory, who must be briefed on his or her continuing responsibility to protect classified information and the sanctions that may follow from the failure to do so. Ultimately, of course, all persons who have not yet signed a nondisclosure agreement will be required to do so as a condition of access to classified information, in accordance with the President's directive of March 11, 1983.

Sincerely,

/s/ Steven Garfinkel
Steven Garfinkel

Name
Title Director Agency
Address
City
State

Pl. Exhibit 10

AFFIDAVIT OF REPRESENTATIVE BARBARA BOXER

I, Barbara A. Boxer, hereby state as follows:

1. I am a United States Representative from California.

2. I am concerned the SF 189 will impede the flow of information to Congress. The word "classifiable" is so broad and vague that it could "arguably" include anything, to use the words of Steven Garfinkel, the Director of the Information Security Oversight Office. In particular, whistleblowers could be held responsible for disclosing information to Congress, even information that is unclassified but might be retroactively designated as classified after the disclosure.

3. SF 189 would almost certainly have a chilling effect on conscientious public servants considering whether to report such matters as waste, fraud, and abuse to Congress, the Inspector General, or any other authorized recipient. This deterrent is particularly dangerous because government employees are already afraid to stick their necks out and risk their careers to make such disclosures. My staff and I have dealt with numerous whistleblowers who have been fearful of the consequences that might flow from their disclosures. Some have required anonymity. I am concerned that the added deterrent of signing SF 189 will silence otherwise well-meaning employees.

4. Without the information provided by federal employees, both Congress and the American people are at a terrible disadvantage. For instance, the House Armed Services Committee depended on candid upfront assessments by military and civilian field personnel in its investigations of problems of both the B-1 Bomber and the MX missile. Likewise, information about faulty and overpriced weapons and spare parts has come from both civilian and military employees of the Department of Defense. In addition, I obtained information from a whistleblower about reservists remaining in Central America for tours that exceeded

the legal time limit on such stays.

5. Although the executive branch provides information to Congress, the information voluntarily provided by the Administration is not sufficient to enable us to fulfill our responsibilities. That information is often one-sided and self-serving and is not sufficient for Congress to probe wrongdoing or mismanagement that the Administration is trying to hide. Whistleblowers often provide leads that direct Congress to a problematic aspect of what may be an otherwise impenetrable subject matter, which is what happened with disclosures about the B-1 Bomber and MX missiles.

6. Although Congress has subpoena power, it would be infeasible for Congress to rely solely on that power to conduct oversight operations. This is because the subpoena enforcement process is rarely invoked, and even then it is long and cumbersome. Subpoenas place the executive and legislative branches at loggerheads and thus heighten the adversarial rather than the cooperative aspects of the relationship, which is counterproductive in the long run.

7. Without the clues that whistleblowers often furnish, Congress would need to commence broad fishing expeditions to uncover matters worthy of more in-depth congressional oversight. It would be both infeasible and inefficient for Congress to ask for everything about the B-1 Bomber program, for example, in an attempt to discover fraud, technical deficiencies, and other problems.

8. Another provision of SF 189 will deter federal employees from providing information to Congress. If an employee provides me with information and I release it, then the employee can be held liable for my actions. In the past, I have served as the intermediary between a whistleblower and the public. For example, after a federal employee gave me information about reservist tours that extended beyond the legal limit, I provided that information to the press. By maintaining his anonymity, I hoped to save the employee from additional adverse job actions.

9. Not only does the Administration view Members of Congress as unauthorized to receive classified information without executive branch approval, but it also seeks to bind us to SF 189. When I sought access to a General Accounting Office report on homeporting from the Department of Energy, I received a letter from Troy E. Wade, Acting Assistant Secretary for Defense Programs, asking me to sign SF 189 as a condition of receiving the report. Although I signed the form in error at the time, I have since revoked my unintended agreement because I do not believe it is appropriate for the executive branch to bind a Member of Congress in this way. Letter to Secretary of Energy John Herrington from Congresswoman Barbara Boxer (October 16, 1987).

Pursuant to 28 U.S.C. § 1746 and Local Rule 106(g), I declare under penalty of perjury that the foregoing is true and correct.

Executed this 17th day of November, 1987.

/s/ Barbara Boxer
Barbara Boxer

Pl. Exhibit 11

[Caption]

AFFIDAVIT OF SENATOR CHARLES E. GRASSLEY

I, Senator Charles E. Grassley, hereby state as follows:

1. I am a United States Senator from Iowa.

2. I am concerned the Standard Form 189 ("SF 189") will deter federal employees from providing information to Congress. The Administration has made it clear that Members of Congress are not authorized to receive "classified or classifiable information," unless high-level agency officials decide that they have a need-to-know that information. Not only will this prior approval requirement deter whistleblowers from providing classified information to Congress as provided for by federal statute, but it will also deter them from communicating a whole range of unclassified information because of the use of the extremely broad and vague concept of "classifiable information."

3. Federal employees provide Members of Congress useful information that may not be forthcoming from the Administration. On one occasion, the Administration would not authorize Air Force Management Systems Deputy A. Ernest Fitzgerald, who had useful and valuable cost information that did not comport with the "official line," to appear at a congressional hearing in his capacity as an official Air Force cost analyst. As the Chairman of the subcommittee holding the hearing, and in order to secure Mr. Fitzgerald's official testimony, I was forced to drive to the Pentagon and personally serve on him a subpoena. On another occasion, I invited Defense Department budget analyst Franklin "Chuck" Spinney to my office to provide me with his defense budget briefing entitled "Plans/Reality Mismatch," since I was deliberating about budget deficit problems as a member of the Senate Budget Committee. At first, then-Defense Secretary Cap Weinberger agreed to allow Mr. Spinney

to brief me. Four days later, he reneged, and I was forced instead to go to extraordinary lengths to secure Mr. Spinney's testimony before an unprecedented joint hearing of the Senate Budget and Armed Services Committees. These examples illustrate the dangers inherent in the executive branch determining whether Congress is authorized to hear from any particular federal employee or to receive any given piece of information.

4. Although I endorse legitimate attempts by any branch of government to prevent disclosures of properly classified information the disclosure of which could harm national security, I have concluded based on my personal involvement and dealings with executive branch officials on this matter that SF 189 is an attempt to go way beyond the legitimate protection of classified information.

5. Over the past several months, I have negotiated with officials of different agencies and the White House to work out a reasonable definition of the term "classifiable." I sought to replace the Federal Register definitions with narrower language taken directly from a fact sheet issued by the Information Security Oversight Office. That language defines "classifiable" as

> unmarked information that already is classified, or meets the standards for classification and is in the process of being classified. It does not refer to unclassified information that might, perchance, be classified sometime in the future. The only fact pattern in which an employee might be held liable for disclosing unclassified information could occur when the employee knows, or reasonably should know, that the information is in the process of a classification determination and requires interim protection as provided in Section 1.1(c) of Executive Order 12356.

Although the term "unmarked classified information" is inherently contradictory because classified information is by definition marked as such under the terms of the controlling Executive

Order, the latter part of this definition would prevent officials from classifying information in order to retaliate against whistleblowers who reveal the information when it is not classified.

6. However, the Administration reneged on its initial acceptance of this narrower definition, leaving me to wonder whether the Administration wants the latitude afforded by this vague term, which I believe threatens both the First Amendment and statutory rights of federal employees and the rights of Congress to receive information.

7. During the past week, Administration officials have indicated that they are interested in reopening negotiations. I have directed them to appropriate congressional channels so that future negotiations will proceed in a more accountable manner.

Pursuant to 28 U.S.C. § 1746 and Local Rule 106(g), I declare under penalty of perjury that the foregoing is true and correct.

Executed this 18th day of November, 1987.

/s/Chuck Grassley
Charles E. Grassley

Def. Exhibit 4

[Caption]

DECLARATION OF WILLIAM H. WEBSTER
DIRECTOR OF CENTRAL INTELLIGENCE

I, William H. Webster, declare as follows:

1. I am the Director of Central Intelligence (DCI), and have served as DCI since 26 May 1987. As the DCI, I am the head of the Central Intelligence Agency. In my current position I also serve as the primary advisor to the President of the United States on matters of national foreign intelligence, and I am responsible for coordinating the national intelligence activities of the civilian and military departments, agencies, and elements comprising the United States Intelligence Community.

2. I understand that I have been named as a defendant, in my official capacity, in the above-captioned action. I also understand that the plaintiffs are seeking a preliminary injunction against continued use of Form 4193 on the ground that the use violates recent legislation. I am submitting this declaration in support of the defendants' opposition to plaintiffs' motion for a preliminary injunction and pursuant to my duties as DCI as set forth in the National Security Act of 1947, 50 U.S.C. § 402, et seq. and Executive Order 12333, entitled "United States Intelligence Activities."

3. Section 102(d)(3) of the National Security Act of 1947, 50 U.S.C. § 403(d)(3), and section 1.5(h) of Executive Order 12333 provide that the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure. Certain classified information relating to intelligence sources and methods is so sensitive that it must be placed within special access programs to control access to, distribution and protection of such information. This type of information is referred to as Sensitive Compartmented Informa-

tion (SCI). Under the authority of the National Security Act, Executive Order 12333, and Section 4.2(a) of Executive order 12356, entitled "National Security Information," I have the responsibility for the creation of special access programs pertaining to intelligence activities, sources and methods. The SCI security system was established in fulfillment of this responsibility. As I will describe, Form 4193, entitled "Sensitive Compartmented Information Nondisclosure Agreement," is an integral part of the security system established to protect intelligence sources and methods relating to SCI.

4. Generally speaking, SCI consists of data describing sophisticated technical systems for collecting intelligence and the information collected by those systems. Because of the extreme sensitivity of this information and material, SCI requires special controls for restricted handling within designated compartments. These compartments provide extraordinary security protection for those intelligence activities that, if comprised, could reasonably be expected to cause severe harm to the national security. The nature, sensitivity and fragility of SCI is described in the report of the DCI Security Committee, attached hereto as Exhibit A and entitled "Sensitive Compartmented Information: Characteristics and Security Requirements."

5. Pursuant to my responsibilities under the National Security Act, Executive Order 12333, and Executive Order 12356, I have promulgated standards governing access to SCI, including the requirement that Form 4193, or an equivalent nondisclosure form, be signed as a condition of personal access to SCI. Prior to 22 December 1987, Government employees and contractor personnel seeking access to SCI were required to sign the Form 4193 or an equivalent form. Since 22 December 1987, I have required Government employees and contractor personnel who access to SCI to sign the Form 4193 and an addendum that states that Form 4193 will be implemented and enforced in a manner consistent with 630 of the Treasury, Postal Service and General Government Appropriations Act, 1988, as incorporated in the

Omnibus Continuing Appropriations Resolution for Fiscal Year 1988, Pub. L. No. 100-202 and applicable law. I was advised by my Office of General Counsel that use of this addendum in conjunction with Form 4193 was an appropriate means, consistent with law, to ensure continued protection of SCI. The Office of Legal Counsel of the Department of Justice concurred with this view.

6. My staff is currently considering modifications of the Form 4193 in light of the new legislation. If approved, a new form will be distributed to all agencies and departments currently using the Form 4193 accompanied by the addendum. In the interim, however, it is essential to continue to use the current Form 4193 in a manner consistent with the law and my responsibility to protect SCI. As discussed below, Form 4193 contains a number of provisions which aid me in fulfilling this responsibility.

7. The form establishes a precise contractual relationship between the United States Government and an individual granted access to SCI. Remedies for violating the obligations imposed by this agreement may include damages, injunctive relief, and the imposition of a constructive trust. If the Government could not use the Form 4193, accompanied by the addendum, I believe that this could create severe difficulties in my ongoing efforts to protect SCI from unauthorized disclosure. This is so for several reasons. First, SCI would no longer be protected by the form's pre-publication review provision. This key pre-publication review provision ensures that persons with access to SCI seek review of certain designated material that they intend to provide to unauthorized persons or the public. Absent this provision, the Government could not require review of material that might contain SCI prior to the actual disclosure. In other words, a person with access to SCI would be under no obligation to receive approval prior to publication. If the Government wished to take action against such disclosures, the Government would be forced to wait until the disclosures took place. Pursuit of that remedy could require the Government to confirm the informa-

tion, thereby damaging intelligence sources and methods and possibly compounding that damage through additional disclosures. For these reasons, the pre-publication review feature is a critical component of Form 4193 and of the SCI security program. If continued use of Form 4193 with the addendum were enjoined, the pre-publication review clause would also necessarily fail, significantly impairing my ability to protect SCI.

8. Second, there is a strong need for the personal obligations established by the Form 4193. Without the discipline and protection afforded by these obligations, there is a greater opportunity and risk for inadvertent or even deliberate disclosure of SCI. The remedies granted by the courts thus far for violating the obligations contained in similar agreements have created strong disincentives for people to violate their agreements and have greatly lessened the risk of compromising classified information. Equally important, Form 4193 and equivalent forms underscore on an individual level the importance of protecting SCI and have sensitized individuals of their personal obligations to protect SCI on a daily basis.

9. As the attached report indicates, a large number of people are needed to develop, build, and operate SCI systems and to analyze the SCI material collected. Thus, there is a great risk of unauthorized disclosure of SCI. Safeguards are essential to protect against such disclosures and the potential countermeasures of foreign intelligence services. Such safeguards are essential for me to function effectively in my role as DCI and to provide the necessary, timely dissemination of sensitive intelligence to U.S. policymakers.

10. The need for special measures, including Form 4193, to protect SCI is also dictated by the need to protect the special systems involved. The compromise of an SCI technical system could be devastating and could result in the unavailability of critical intelligence. Such a severe compromise might also mean loss of valuable intelligence about "denied areas" (i.e., intelligence information not available by any other means) and could

require the development of completely new, extremely expensive, state-of-the-art systems. Additionally, if an SCI system is compromised, hostile intelligence services have the option of running deception operations—such as providing misleading data which may result in flawed U.S. foreign and defense policies or decision.

11. Another significant harm that could result from the inability to use the form is the impairment of our damage assessment capability for the unauthorized disclosure of SCI. The form presently represents a primary means for the Government to keep track of individuals possessing SCI access. This tracking system often enables the Government to determine who had access to the SCI disclosed at the time of the compromise and thus, who could have made the unauthorized disclosure. Clearly, this ability is needed to monitor disclosures, intentional or otherwise, of SCI.

12. In summary, Form 4193 with the addendum is a valuable part of the Government's ongoing efforts to protect SCI from unauthorized disclosure. As previously stated, the approval and possible distribution of a new form is currently being considered. In the interim, I submit that the enjoining of this form could cause great difficulties for me in carrying out my responsibilities to protect intelligence sources and methods, and particularly SCI, from unauthorized disclosure.

13.I declare under penalty of perjury that the foregoing is true to the best of my knowledge and belief.

/s/William H. Webster
William H. Webster
Director of Central Intelligence

Date: 1 March 1988

EXHIBIT A IN SUPPORT OF THE DECLARATION OF WILLIAM H. WEBSTER

Director of Central Intelligence
DCI

Sensitive Compartmented Information:
Characteristics and Security
Requirements

Prepared by
The
Security
Committee

June 1984

Preface

This paper on the nature of sensitive Compartmented Information (SCI) and pertinent controls was originally produced at the CONFIDENTIAL level in March 1984. It was intended for background use by legislative liaison officers responding to Congressional inquiries about SCI security requirements. It has been redrafted for issuance as an unclassified text because SCI security recently has become a matter of interest to all three branches of Government. The concept of providing special systems of compartmented protection to entire programs of intelligence collection and production is not widely known or understood. This paper is intended to assist those who must officially consider various aspects of SCI without the benefit of extensive experience with these programs.

In the continuing discussions of the appropriate security measures for protecting Sensitive Compartmented Information (SCI), including polygraph examinations and nondisclosure agreements, there has been little or no attention to what SCI is. These discussions raise issues about SCI which include:

> Does the nature of SCI lend itself to varying levels and kinds of security protection? Is the SCI accessed by "consumers" essentially different from the SCI dealt with by "producers"? Should some individuals be subject to stricter security screening for SCI access than others? Should the personnel of agencies not engaged in collecting or producing intelligence meet the same security standards for SCI access as those of intelligence agencies? Should political appointees be required to protect SCI from disclosure in the same manner as career federal employees? Are those who are granted access to SCI required to meet a higher standard of personnel security than those cleared for non-compartmented Confidential, Secret or Top Secret Information? Is there a different assessment of acceptable risk in the SCI systems than for other classified information?

This report attempts to describe what SCI is, why it is sensitive, why the revelation of SCI that an unwary individual might consider insignificant or trivial can be damaging to an entire program for SCI collection, and why we should not be willing to accept any perceptible level of risk in decisions on personnel being granted access to SCI.

Sensitive Compartmented Information is data about sophisticated technical systems for collecting intelligence and the information collected by those systems. The characteristics of the systems that necessitated the development of SCI programs are (a) that compared to conventional intelligence activities employ-

ing human sources, many more people normally must know sensitive information in order to develop, build, and operate the systems and to analyze the material they collect; (b) that they generally produce large quantities of accurate, detailed intelligence, which is needed and relied upon by senior planners and policymakers, and which, by its nature, is extremely fragile, in that it reveals the characteristics of the systems that collect it; and (c) that they are extremely vulnerable to adversary countermeasures, i.e., denial or deception.

Most people can easily understand the need for tight security in classic espionage operations employing live agents. The need for strong security is dictated by the need for source protection and, of course, it is clear that the apprehension of an agent results in the loss of valuable intelligence. The neutralization of a technical collection system is more akin to the loss of a whole agent network than to the loss of a single agent and the loss of such systems has severe consequences. These include the loss of valuable intelligence about "denied areas" which is not available by any other means; the cost of developing and producing new technical collection systems, which are extremely expensive, state-of-the-art programs; and the risks to the national security attendant to a lack of knowledge of what our adversaries are up to.

Communications intelligence, as defined by 18 U.S.C. 798, is the classic example of SCI, and normally is derived from intercepted communications. The unauthorized disclosure of such intelligence can reveal to the target country which of its messages are being intercepted and which ones are being read. If the targeted country takes the clearly indicated countermeasures, no further intelligence can be expected from that source and by that method. Similarly, the compromise of other technical collection systems, or intelligence derived from them, can tell our adversaries the capabilities of the systems and how to

take countermeasures. Even worse, once the target country's government knows what the systems collect and how it is collected, it has the option of conducting deception operations, i.e., providing misleading data which may result in defective U.S. foreign and defense policies.

To guard against these risks, SCI security control systems have been evolved in the years since World War II, when the Japanese and German cryptographic systems were broken by the Allies, furnishing intelligence which was vital to victory over the Axis Powers. In structuring these systems, the lessons of Pearl Harbor have been borne in mind ... the systems must permit timely dissemination of sensitive intelligence to those who need it to guide and carry out U.S. defense and foreign policy. Over the years, it has been demonstrated that the recipients' confidence in intelligence reporting has a direct relationship to the recipients' knowledge of the source or method producing it. Because of the amount of intelligence produced by the SCI systems and its broad utility, those with access to SCI number in the thousands.

The authority for SCI control systems is based upon the statutory responsibility of the Director of Central Intelligence (DCI), under the National Security Act of 1947, for the protection of intelligence sources and methods, and upon Executive Order 12356, which authorizes him to create special access programs for especially sensitive intelligence activities.

SCI systems, therefore, cover activities and information of extraordinary sensitivity and fragility from a security standpoint. They serve to restrict access to the protected information to persons who (a) have a clearly established official need for that information, and (b) who meet more rigorous and stringent personnel security criteria. Persons cleared for Confidential, Secret, or Top Secret information are not automatically eligible

by virtue of those clearances for access to SCI.

The personnel security criteria for access to all SCI are established by the DCI and are promulgated in Director of Central Intelligence Directive 1/14. Comparatively, the criteria for TS clearance require that denial be based upon a well-defined character or personality defect posing a threat to the national security. Because of the vulnerabilities and susceptibilities of SCI programs, special judgments must be made. In effect, no risk is tolerable where SCI is involved, and individuals who have been granted Top Secret clearances may be denied approval for access to SCI. Just as clearance for Top Secret does not automatically guarantee SCI access approval, the denial of SCI approval does not necessarily mean denial or revocation of TS clearance. This reflects the difference in the way SCI security is managed, and that it involves a higher order of security than non-SCI security.

SCI security control systems depend upon distinctive markings and restricted handling of material, stricter personnel security processing for access, and holding SCI material in "control centers" with physical and procedural barriers to preclude access by those who have not been formally approved. The SCI control systems provide an organized program for predetermining a generalized need-to-know regarding specific categories of intelligence and/or sources and methods employed in their collection.

Everyone authorized access to SCI, regardless of that persons' function, receives information that, if revealed to an unauthorized person, can compromise the system and reveal ways of countering it. Because the intelligence inherently is source-revealing, the reader of an SCI intelligence report is just as capable of revealing compromising data about a system as the builder or operator of the system. Material collected by SCI

systems which does not reveal the characteristics and vulnerabilities of the source is considered to be sanitized and is disseminated outside compartmented channels.

In accepting sensitive compartmented information, the recipient accepts the accompanying responsibilities and restrictions in a most explicit way. Each individual approved for access is indoctrinated on the extreme vulnerabilities of the collection systems, the risk to the systems of the unauthorized disclosure of the intelligence they collect, and the rules for safeguarding SCI. As a condition of access, the newly approved individual signs an agreement to abide by the security rules for SCI.

To summarize, the rationale for SCI control systems includes the following concepts:

— Sources and methods producing quantities of high quality intelligence, which are extremely vulnerable to countermeasures, require an extraordinary degree of security protection.

— Extraordinary protection can be afforded by restricting knowledge of these sources and methods and, where necessary, the intelligence they produce, to persons who have been subjected to especially thorough security screening, whose knowledge of such information is required for performance of functions essential to the national security, and who have entered into an agreement requiring that they protect these sources and methods in the manner prescribed by the U.S. Government.

— Because of the extreme vulnerability to countermeasures of the operations covered by SCI control systems, persons granted access to SCI must be determined by thorough investigation to be reliable and trustworthy. The objective of personnel security determinations for SCI access should be

a risk-free population of approved individuals. Therefore, a substantially more vigorous personnel screening process is necessary and a determination standard beyond that for other classified information must be used.

— Especially restricted channels are required for the transmission and use of data revealing the sensitive nature of these sources and methods, and of derived intelligence having the innate capability to compromise such data.

— Regardless of how carefully the security system is structured, the security of our secrets depends, in the final analysis, upon every person granted access. If any of those entrusted with these secrets has vulnerabilities or susceptibilities which may be exploited, then our security can be breached. Every effort must be expended to avoid such an occurrence.

[Caption]

DECLARATION OF LT. GENERAL EDWARD J. HEINZ

I, LT. GENERAL EDWARD J. HEINZ, USAF, declare as follows:

1. I am the Director of the Intelligence Community Staff, which is a staff element of the Director of Central Intelligence (DCI). I have previously executed a declaration in this litigation on 9 February 1988.

2. Pursuant to Section 102(d)(3) of the National Security Act of 1947, 50 U.S.C. § 403(d)(3), and Executive Order 12356, the DCI is responsible for promulgating policies and procedures for the security, use, and dissemination of Sensitive Compartmented Information (SCI) government-wide. SCI, which generally consists of data describing sophisticated technical systems for collecting intelligence and the information collected by those systems, is some of the Nation's most sensitive intelligence information and material and, therefore, it requires special controls for restricted handling within designated compartments. Further information concerning SCI is set forth in the Declaration of DCI Webster dated 1 March 1988.

3. In my capacity as Director of the Intelligence Community Staff, I am responsible for assisting the DCI in establishing security policy with respect to SCI. The DCI has directed that the signing of a DCI-authorized nondisclosure agreement is a condition of access to SCI. On 18 March 1988, the SCI approved the issuance of Form 4355 (attached as Exhibit A) as the new SCI nondisclosure agreement, replacing Form 4193. As directed by the DCI, I notified appropriate senior officials in the Intelligence Community to discontinue use of Form 4193, or equivalent nondisclosure agreements, and to implement the new Form 4355, or an equivalent nondisclosure agreement, in its place. (A copy of my memorandum containing such instructions is attached hereto as exhibit B). It is my understanding that the DCI's

Special Security Center has informed the appropriate nonintelligence agencies of this change. (A copy of one of the notification memoranda is attached hereto as exhibit C).

4. I declare under penalty of perjury that the foregoing is true to the best of my belief.

/s/ Edward J. Heinz
EDWARD J. HEINZ
LT. GENERAL, USAF

Date: 24 March 1988

EXHIBIT A IN SUPPORT OF LT. GENERAL HEINZ'S DECLARATION

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States

(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in the process of a classification under the standards of Executive Order 12356 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to

advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might by SCI, or related or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency

that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon them, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798 and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials, which may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12356, as

amended, so that I may read them at this time, if I so choose.

FORM 4355
3/88

(Replaces Form 4193 which is obsolete and will not be used)

Pl. Exhibit 16

THE WHITE HOUSE
Washington

RECEIVED
MAR 1988
HOUSE COMMITTEE ON
GOVERNMENT OPERATIONS

March 8, 1988

Dear Chairman Brooks:

On February 9, you inquired about the National Security Council (NSC) staff's practices under Section 630 of Public Law 100-202, the Continuing Resolution for Fiscal Year 1988, which placed certain restrictions on the use of nondisclosure forms.

After December 22, 1987, and consistent with guidance from the Information Security Oversight Office (see Tab A), the NSC staff ceased using Standard Form 189, "Classified Information Nondisclosure Agreement," and Standard Form 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non- Government)."

After December 22, 1987, and consistent with guidance from the Central Intelligence Agency (see Tab B), the NSC staff continued to use Form 4193 together with the following addendum:

> The obligations imposed by this Agreement shall be implemented and enforced in a manner consistent with the section entitled "Employee Disclosure Agreements" contained in P.L. 100-202, Continuing Appropriations for Fiscal Year 1988, 22 December 1987, and other applicable law.

The NSC staff also has continued to use a third nondisclosure form (based on Form 4193) for NSC special access programs (see Tab C). In response to the Continuing Resolution, this form was modified: the words "classifiable under" were replaced with "otherwise meets." We believe that this change fully complies with the Continuing Resolution. In order to eliminate any possible misunderstanding, however, we recently further modified the form by replacing the words "classified or classifiable" with language tracking Section 630: "marked as classified, unmarked but which I know to be classified, or unclassified which I know to be in the process of a classification determination" (see Tab D). The NSC staff now uses this version of the form.

Sincerely,

/s/ Colin L. Powell

[Attachments]

The Honorable Jack Brooks
Chairman, Committee on Government Operations
U.S. House of Representatives
Washington, D.C. 20515

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

NATIONAL FEDERATION OF FEDERAL EMPLOYEES, *Plaintiff,*	)	Civil Action No. 87-2284-OG
v.	)	
UNITED STATES OF AMERICA, *et al.*, *Defendants.*	)	**FILED JUL 29, 1988 Clerk, U.S. District Court District of Columbia**
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, *et al.*, *Plaintiffs,*	)	Civil Action No. 87-2412-OG
v.	)	
STEVEN GARFINKEL, *et al.*, *Defendants.*	)	

FINAL JUDGMENT AND ORDER

Upon consideration of defendants' Motion to Dismiss and plaintiffs' Motions for Summary Judgment, the oppositions thereto, and the record herein, and for the reasons stated in the accompanying memorandum, it is by the Court this *28th* day of July, 1988

ORDERED that defendants' Motion to Dismiss be, and hereby is, granted as to counts V and VII in Civil Action No. 87-2412 and denied as to the remaining counts; and it is further

ORDERED that plaintiffs' Motions for Summary Judgment be, and hereby are, granted, in part, as to count II in Civil Action No. 87-2284 and as to counts I and II in Civil Action

No. 872412, and denied as to all remaining counts; and it is further

ADJUDGED AND DETERMINED that use of the term "classifiable" in SF 189, SF 4193, DD 1847-1, or any other nondisclosure agreement is unconstitutional unless the form includes or is accompanied by the definition of "classifiable" that appears in 32 C.F.R. § 2003.20(h)(1); and it is further

ADJUDGED AND DETERMINED that an agreement includes or is accompanied by the definition of "classifiable" that appears in 32 C.F.R. § 2003.20(h)(1) if this section of the C.F.R. is reprinted and:

(1) Presented to the employee at the time the agreement is executed; or

(2) Delivered within sixty (60) days of the date of this Order to the employee who has already signed the agreement; and it is further

ORDERED that until the employee receives a copy of the definition of "classifiable," the nondisclosure agreement may not be enforced to penalize the employee for disclosure of "classifiable" information; and it is further

ORDERED that in lieu of delivery or presentment of the definition of "classifiable," the Information Security Oversight Office, the Director of Central Intelligence, the Department of Defense, and any other agency that has used a nondisclosure agreement containing the word "classifiable" may notify every employee that has signed such an agreement that "classifiable" is stricken from the agreement and that liability shall not arise under the agreement for disclosure of "classifiable" information; and it is further

ORDERED that within sixty (60) days of the date of this Order each employee that has signed a nondisclosure agreement containing the word "classifiable" shall receive a copy of the definition of "classifiable" that appears in 32 C.F.R. § 2003.20(h)(1) or notice that the word is stricken from the agreement and shall not be a basis for liability.

/s/ **Oliver Gasch**

United States District Judge
Oliver Gasch

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

NATIONAL FEDERATION OF FEDERAL EMPLOYEES, *Plaintiff,*	)	Civil Action No. 87-2284-OG
v.	)	
UNITED STATES OF AMERICA, *et al.*, *Defendants.*	)	**FILED SEP 26, 1988 Clerk, U.S. District Court District of Columbia**
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, *et al.*, *Plaintiffs,*	)	Civil Action No. 87-2412OG
v.	)	
STEVEN GARFINKEL, *et al.*, *Defendants.*	)	

ORDER

Upon consideration of the defendants' motion to alter or amend judgment, the oppositions thereto, and the record herein, and it appearing from the representations of government counsel in open court that the word "classifiable" has been deleted in some instances and other words substituted therefor; and it further appearing that to the extent that "classifiable" is still deemed binding on certain government employees, that those who are deemed bound by the non-disclosure agreement be given actual notice as hereinafter provided, it is by the Court this *25th* day of September, 1988,

ORDERED, that defendants' motion be, and hereby is, granted in part and denied in part; and it is further

ORDERED that the defendants are granted an additional thirty (30) days within which to comply with this Court's Order of July 29, 1988, so that within ninety (90) days of the date of the Court's original Order, each employee who has signed a nondisclosure agreement containing the word "classifiable" shall either receive a copy of the definition of "classifiable" as the same appears in 32 C.F.R. § 2003.20(h)(1) or notice that the word has been stricken from the agreement and what, if any, words have been substituted in lieu thereof.

/s/ **Oliver Gasch**

Judge

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such classified informa-

tion to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798 and *952 of Title 18, United States Code, *Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, Executive Order 12356 or its successor, and Section 2003.20, Title 32, Code of Federal Regulations, so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NO. (See notice below)

ORGANIZATION (IF CONTRACTOR, LICENSEE OR AGENT, PROVIDE: NAME, ADDRESS AND, IF APPLICABLE FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS

THE EXECUTION OF THIS AGREEMENT WITNESSED BY THE UNDERSIGNED.

SIGNATURE	DATE

NAME AND ADDRESS (Type or print)

ACCEPTANCE

THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT

SIGNATURE	DATE

NAME AND ADDRESS (Type or print)

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that all federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT

STANDARD FORM 312 (9/88)
Prescribed by GSA/ISOO
32 CFR 2003:E.O. 12356